REMARKS

Claims 1, 2, 4, 5, 10, 11 and 16-24 are amended to correct formality errors and to more clearly define the invention.

Support for the amendments is found in the existing claims and in the Application description in connection with Figure 2 on pages 10-13 and specifically on page 14 lines 32-36 and other places.

I. Objection to claims.

Claim 10 is objected because of informalities. Specifically the claim ends with "session identifier; and".

Claim 10 is amended to remove the informality. Consequently this ground of objection is no longer deemed to apply and its withdrawal is respectfully requested.

II. Rejection of claims 4, 18 and 24 *under 35 USC 112.*

Claims 4, 18 and 24 are rejected under 35 USC 112 second paragraph as being indefinite for failing to particularly point out and distinctly claim the subject matter. Specifically, claim 4 states that the URL processor "processes a URL link to a second application differently to a link to a web page provided by said first application". Similarly claims 18 and 24 state that a URL processor generates "a URL link to a second application differently to a URL link to a web page provided by said first application". These limitations are rejected as being vague as it is unclear exactly in what ways the processing and generating are done differently.

Claims 4, 18 and 24 are amended to recite the ways the processing and generating are done differently. Specifically, claim 4 recites "a URL processor for adaptively processing a URL link to a second application differently to an intra-application link to a web page provided by said first application *by using said received encryption key to encrypt a URL link address portion* of said URL link to said second application to produce a processed URL and by *non-encryption* of said intra-application link". Similar amendments are made to claims 18 and 24. Consequently this ground of rejection is no longer deemed to apply and its withdrawal is respectfully requested.

III. Rejection under 35 U.S.C. 102(e)

Claims 1-24 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent 6,463,533 – Calamera et al. These claims, as amended, are deemed to be patentable for the reasons given below.

Amended claim 1 recites a system "employed by a first application for encoding URL link data for use in detecting unauthorized URL modification" comprising "an input processor for receiving an encryption key; a URL processor for adaptively processing a URL link to a second application differently to an intra-application link to a web page provided by said first application by using said received encryption key to encrypt a URL link address portion of said URL link to said second application to produce a processed URL and by non-encryption of said intra-application link; and a communication processor for including said processed URL in data representing a web page and for communicating said web page representative data including said processed URL to a requesting application". These features are not shown (or suggested) in Calamera.

The system of claim 1 involves "adaptively processing a URL link to a second application differently to an intra-application link to a web page provided by said first application". This is done "by using said received encryption key to encrypt a URL link address portion of said URL link to said second application to produce a processed URL and by non-encryption of said intra-application link". These features address the security deficiencies of URL processing functions of electronic systems. "Applications are vulnerable to the corruption of URL data and the context information conveyed within the URL data. The URL data conveyed from application 200 to application 230 includes context information comprising a session identifier and optionally a user or patient identifier. This URL data is potentially vulnerable to corruption to cause URL replay or redirection of an application to a substitute address or to gain access to application functions and parameters for unauthorized purposes. In order to protect against such corruption and to ensure that the entity being accessed is the one originally targeted, portions of the URL data conveyed between applications are advantageously encrypted" (Application page 11 lines 1-9).

The claimed system addresses the security problem by adaptively generating URLs for accessing intra-application web pages differently to URLs accessing web pages accessed by a different application. See Application page 14 lines 34-36 reciting "because the link to the test results page is an intra-application

link there is no requirement for this particular embedded link to be processed in the manner previously described to incorporate the session identifier and other context information".

Calamera does not show or suggest "adaptively processing a URL link to a second application differently to an intra-application link to a web page provided by said first application". Calamera also fails to show or suggest doing this "by using said received encryption key to encrypt a URL link address portion of said URL link to said second application to produce a processed URL and by non-encryption of said intra-application link". Calamera discloses a generation system that combines a target system (e.g., an Internet website) URL and a current userID into a hashed, encrypted string in order to allow "a computer network site, such as an Internet website, to recognize an anonymous user without revealing the identity of the user" (Calamera column 3 lines 6-10). "In one embodiment of the invention, a one-way hash function is used to generate a site-specific user alias based on the user's identification code and the URL of the website. In an alternative embodiment of the invention, both a one-way hash function and a secret key encryption algorithm are used to generate the site-specific alias" (Calamera column 7 lines 1-7).

In Calamera, a target system, upon receiving a URL request, can use the encrypted string and compare it to some known set of allowable strings in order to identify a user. However the target system cannot decrypt the encrypted string. "Regardless of when the alias is generated or how it is sent to the website accessed by the user, the alias maintains the user's anonymity since it is impractical to determine the user's identity from the alias. Nevertheless, because a user's alias for a particular website does not change over time, the website is able to recognize a particular user from previous occasions when the user accessed the website...Furthermore, since the alias server system can decrypt the alias to determine the user's identity, law enforcement agencies can obtain the user's identity from the operator of the alias server system if necessary" (Calamera column 11 lines 4-16). Consequently, the target system is unable to decrypt (nor has access to the necessary key for decrypting) the encrypted string. Only the source (alias server) system is able to decrypt.

In contrast, in the claimed arrangements, a target system has access to the key used by the generation system so that the data can be decrypted. Additional contextual data to be used by the target system (e.g. patient identifier, encounter identifier, and so on) can be included in the encrypted string for use by the target system. In the Calamera system such information cannot be conveyed for decryption

and subsequent use. Calamera also has no notion of session. In contrast to the claimed system, the Calamera system does NOT convey information in URL data fields for subsequent decryption and use by a target system.

Calamera does not show or suggest "adaptively processing a URL link to a second application differently to an intra-application link to a web page provided by said first application". Calamera also fails to show or suggest doing this "by using said received encryption key to encrypt a URL link address portion of said URL link to said second application to produce a processed URL and by non-encryption of said intra-application link". Calamera provides no suggestion of such an adaptive URL processing system using "encryption" and "non-encryption" based on whether a URL accesses an intra-application web page or not. Calamera uses fixed encryption systems. Specifically, "In one embodiment of the invention, a one-way hash function is used to generate a site-specific user alias based on the user's identification code and the URL of the website. In an alternative embodiment of the invention, both a one-way hash function and a secret key encryption algorithm are used to generate the site-specific alias" (Calamera column 7 lines 1-7). Further, since the purpose of the Calamera encryption system is to allow "a computer network site, such as an Internet website, to recognize an anonymous user without revealing the identity of the user", there is nor reason, problem recognition or motivation for amending the Calamera system to include the claimed arrangement (Calamera column 3 lines 6-10). Consequently, withdrawal of the rejection of amended claim 1 under 35 USC 102(e) is respectfully requested.

Amended dependent claim 2 is considered to be patentable based on its dependence on claim 1. Claim 2 is also considered to be patentable because Calamera does not show (or suggest) use of an "encryption key...accessible by said first and second applications from a managing application". Calamera does not provide an "encryption key...accessible by said first" (source application) and a "second" target application as this would enable a target system access to a user's identity information and undermine the purpose of the Calamera system. In Calamera, a target system, upon receiving a URL request, can use the encrypted string and compare it to some known set of allowable strings in order to identify a user. However the target system cannot decrypt the encrypted string. "Regardless of when the alias is generated or how it is sent to the website accessed by the user, the alias maintains the user's anonymity since it is impractical to determine the user's identity from the alias" (Calamera column 11 lines 4-16). Consequently, the target system is unable to decrypt (nor has

access to the necessary key for decrypting) the encrypted string. Only the source (alias server) system is able to decrypt.

Dependent claim 3 is considered to be patentable based on its dependence on claim 1. Claim 3 is also considered to be patentable because Calamera does not show (or suggest) the "communication processor communicates said URL link address portion to a managing application for encryption". Calamera does not suggest such a separate managing application used for encryption of URL data and operating in conjunction with distinct "first and "second" applications. Calamera in column 8 lines 43-46 relied on in the Rejection mentions an Alias server system for providing a site specific user alias generated by a 3 step process but provides no suggestion of just receiving "URL link address portion" for encryption operating in conjunction with distinct "first and "second" applications.

Amended dependent claim 4 is considered to be patentable based on its dependence on claim 1. Claim 4 is also considered to be patentable because Calamera does not show (or suggest) the "URL processor of said first application adaptively processes said URL link to said second application differently to said link to said web page provided by said first application in response to an identified URL type". As previously explained in connection with Figure 1 Calamera does not suggest adaptive URL encryption at all.

Amended dependent claim 5 is considered to be patentable based on its dependence on claims 1 and 4. Claim 5 is also considered to be patentable because Calamera does not show (or suggest) "said URL link to said second application includes an encrypted address portion and said link to said web page provided by said first application includes a non-encrypted address portion". Calamera does not suggest such a feature combination for reasons given in connection with claim 1.

Dependent claim 6 is considered to be patentable based on its dependence on claim 1. Claim 6 is also considered to be patentable because Calamera does not show (or suggest) "a browser application for providing a user interface display permitting user entry of identification information and for providing user identification information to said first application wherein said first application authenticates said user identification information prior to permitting user access to functions of said first application". Calamera does not suggest such a feature combination for reasons given in connection with claim 1.

Dependent claim 7 is considered to be patentable based on its dependence on claim 1. Claim 7 is also considered to be patentable because Calamera does not show (or suggest) "said URL processor compresses said URL link address portion and encrypts a compressed URL link address portion". Calamera does not suggest such a feature combination for reasons given in connection with claim 1.

Dependent claim 8 is considered to be patentable based on its dependence on claims 1 and 7. Claim 8 is also considered to be patentable because Calamera does not show (or suggest) "said URL processor compresses said URL link address portion using a hash function". Calamera does not suggest such a feature combination for reasons given in connection with claim 1.

Dependent claim 9 is considered to be patentable based on its dependence on claims 1 and 7. Claim 9 is also considered to be patentable because Calamera does not show (or suggest) "said communication processor communicates said URL link address portion to a managing application for compression". Calamera does not suggest such a feature combination for reasons given in connection with claim 1.

Amended dependent claim 10 is considered to be patentable based on its dependence on claim 1. Claim 10 is also considered to be patentable because Calamera does not show (or suggest) "said URL processor adaptively generates URL fields including encrypted **patient specific information** for incorporation in said URL link to said second application". Calamera does not suggest such a feature combination for reasons given in connection with claim 1. Specifically, in the Calamera system the target system (Internet web site) is unable to decrypt (nor has access to the necessary key for decrypting) the encrypted string conveyed in a URL. Only the source (alias server) system is able to decrypt the string. In contrast, in the claimed arrangements, a target system has access to the key used by the generation system so that the data can be decrypted. Therefore, additional contextual data to be used by the target system (e.g. patient identifier, encounter identifier, and so on) may be included in the encrypted string for use by the target system. Such information cannot be conveyed for subsequent decryption and use by a target system using the Calamera teaching. Indeed, to allow such decryption is in direct conflict with Calamera's teaching and purpose of enabling "an Internet website, to recognize an anonymous user **without revealing the identity** of the user" (Calamera column 3 lines 6-10).

Amended independent claim 11 recites a "system for encoding URL link data for use in detecting unauthorized URL modification occurring during concurrent operation of a plurality of applications" comprising "a managing application for providing a common encryption key to a plurality of concurrently operating applications; and a first application including, an input processor for receiving said encryption key; a URL processor for adaptively processing a URL link to a second application differently to an intra-application link to a web page provided by said first application by using said received encryption key to encrypt a URL link address portion of said URL link to said second application to produce a processed URL and by non-encryption of said intra-application link; and a communication processor for including said processed URL in data representing a web page and for communicating said web page representative data including said processed URL to a requesting application".

Amended claim 11 is considered to be patentable for the reasons given in connection with claim 1. Claim 11 is also considered to be patentable because Calamera does not show (or suggest) a feature combination including a "managing application for providing a **common encryption key** to a **plurality** of concurrently operating **applications**". In the Calamera system the target system (Internet web site) is unable to decrypt (nor has access to the necessary key for decrypting) the encrypted string conveyed in a URL. Only the source (alias server) system is able to decrypt the string. In contrast, in the claimed arrangements, a target system has access to the key used by the generation system so that the data can be decrypted. Indeed, to allow such decryption is in direct conflict with Calamera's teaching and purpose of enabling "an Internet website, to recognize an anonymous user without revealing the identity of the user" (Calamera column 3 lines 6-10).

Dependent claim 12 is considered to be patentable based on its dependence on claim 11. Claim 12 is also considered to be patentable because Calamera does not show (or suggest) "said communication processor communicates said URL link address portion to a managing application for compression". Calamera does not suggest such a feature combination for reasons given in connection with claim 1.

Dependent claim 13 is considered to be patentable based on its dependence on claim 11. Claim 13 is also considered to be patentable because Calamera does not show (or suggest) "said URL processor compresses said URL link

address portion and encrypts a compressed URL link address portion". Calamera does not suggest such a feature combination.

Dependent claim 14 is considered to be patentable based on its dependence on claims 11 and 13. Claim 14 is also considered to be patentable because Calamera does not show (or suggest) "said URL processor compresses said URL link address portion using a hash function". Calamera does not suggest such a feature combination.

Dependent claim 15 is considered to be patentable based on its dependence on claims 11 and 13. Claim 15 is also considered to be patentable because Calamera does not show (or suggest) "said communication processor communicates said URL link address portion to said managing application for compression". Calamera does not suggest such a feature combination.

Amended independent claim 16 recites a "system for encoding URL link data for use in detecting unauthorized URL modification" comprising "a browser application for providing a user interface display permitting user entry of identification information for providing user identification information to a first application; a first application responsive to said user identification information including, a URL processor for **adaptively generating URL fields** including an encrypted URL address portion and **encrypted patient specific information** for incorporation together with a non-encrypted portion in a processed URL; and a communication processor for including said processed URL in data representing a web page and for communicating said web page representative data including said processed URL to a requesting application". Amended claim 16 is considered to be patentable for the reasons given in connection with claims 1 and 10.

Amended dependent claim 17 is considered to be patentable based on its dependence on claim 16. Claim 17 is also considered to be patentable because Calamera does not show (or suggest) "said communication processor communicates said URL address portion and said **encrypted patient specific information** to another application for encryption". Calamera does not contemplate or mention encrypting **"patient specific information"** within a URL at all.

Amended independent claim 18 recites a "system for encoding URL link data for use in detecting unauthorized URL modification" comprising "a browser application for providing a user interface display permitting user entry of

identification information for providing user identification information to a first application; a first application responsive to said user identification information including, a URL processor for **adaptively generating URL fields** including an encrypted URL address portion and **encrypted patient specific information** for incorporation together with a non-encrypted portion in a processed URL; and a communication processor for including said processed URL in data representing a web page and for communicating said web page representative data including said processed URL to a requesting application". Amended claim 18 is considered to be patentable for the reasons given in connection with claim 1.

Amended dependent claim 19 is considered to be patentable based on its dependence on claim 18. Claim 19 is also considered to be patentable because Calamera does not show (or suggest) generation of "a URL field including **encrypted patient specific information** for incorporation in said generated URL link to said second application". Calamera does not convey encrypted data in a URL for later decryption at all as explained in connection with claim 10.

Amended independent claim 20 recites a "A system supporting concurrent operation of a plurality of Internet compatible applications" comprising "a browser application including, a display generator for providing a user interface display permitting user entry of identification information and commands for a plurality of Internet compatible applications and for providing user identification information to a first application; a URL generator for adaptively generating a URL including URL fields incorporating an encrypted URL address portion and a non-encrypted session identifier; and a processor for initiating communication of said generated URL to said first application in response to validation of said user identification information, said first application having access to a key for decrypting said encrypted URL address portion". Amended claim 20 is considered to be patentable for reasons given in connection with claim 1. Claim 20 is also considered to be patentable because Calamera does not show (or suggest) a "URL generator for adaptively generating a URL including URL fields incorporating an encrypted URL address portion and a **non-encrypted session identifier**" for "communication" to a "first application...having access to a key for decrypting said encrypted URL address portion". In the Calamera system the target system (Internet web site) is unable to decrypt (nor has access to the necessary key for decrypting) the encrypted string conveyed in a URL. Only the source (alias server) system is able to decrypt the string. In contrast, in the claimed arrangements, a target system has access to the key used by the generation system so that the data can be decrypted. Further, Calamera does not

contemplate or mention "session" in column 8 lines 52-60 or elsewhere, contrary to the Rejection statement on page 6.

Amended independent claims 21-23 are considered to be patentable based for reasons given in connection with claim 1.

Amended independent claim 24 is considered to be patentable for reasons given in connection with claims 1 and 20. Consequently, withdrawal of the rejection of claims 1-24 under 35 USC 102(e) is respectfully requested.

In view of the above amendments and remarks, Applicants submit that the Application is in condition for allowance, and favorable reconsideration is requested.

Respectfully submitted,

Date: November 30, 2004

Alexander J. Burke
Reg. No. 40,425

Alexander J. Burke
Intellectual Property Department
Siemens Corporation,
170 Wood Avenue South
Iselin, N.J. 08830
Tel. 732 321 3023
Fax 732 321 3030